APPLICATION

FOR

UNITED STATES LETTERS PATENT

APPLICANT(S) NAME: T. Hahn

TITLE: System And Method For Granting Access To Resources

DOCKET NO. END920010126US1

INTERNATIONAL BUSINESS MACHINES CORPORATION

Certificate of Mailing Under 37 CFR 1.10

I hereby certify that, on the date shown below, this correspondence is being deposited with the United States Postal Service in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C., 20231 as "Express Mail Post Office to Addressee".

"Express Mail" Label Number EL598672395

On January 11, 2002

June Mitchell

Typed or Printed Name of Person Mailing Correspondence

June Mitchell 1/11/02

Signature of Person Mailing Correspondence *Date*

SYSTEM AND METHOD FOR GRANTING ACCESS TO RESOURCES

Background of the Invention

The invention relates generally to computer systems and deals more particularly with a system and method for determining which resources a user can access.

In many computing systems, there is a need to determine whether a user who is requesting information or some other resource is allowed to access the resource. A common technique to determine whether the user is allowed to access the resource involves authentication and authorization. Authentication is the process of determining whether the requesting user is, in fact, the user that has been represented by the user. This is typically done by comparing the ID and password submitted by the user to entries in an authentication table to determine if they match. The ID submitted by the user can be an ID associated with the user as an individual or an ID associated with a group in which the user is a member. Authorization is the process of determining whether the authenticated user or group has been granted access (i.e. has been authorized) to access the resource that has been requested. The authorization system indicates which resources each individual user is permitted to access and which resources each group is permitted to access. These authorizations may have been assigned previously by a system administrator to control access to sensitive or restricted resources. It is common for authentication and authorization to be handled as separate steps, although in most cases the authentication system is closely tied to the authorization system.

Some times, the same user has different user IDs or can gain access through a group ID for a group in which the user is a member. Each different user ID can be permitted to access different resources. For example, Mr. Jones as an individual can be granted access to resource X via one user ID and Mr. Jones as an individual can be granted access to resource Y via a different user ID. Also, Mr. Jones as part of a group can be granted access to resources Z via another

group ID. Thus, the resources that a given user is permitted to access depends on what ID the user submits with his or her request. While such a technique is effective in controlling access to sensitive or restricted resources, a single person may need to make multiple requests with multiple IDs to access all the resources that the person is permitted to access.

Accordingly, an object of the present invention is to simplify the authorization process for a user to access different resources where the user has or can use more than one ID and each ID alone is not granted authority to access all of these resources.

Summary of the Present Invention

The present invention resides in a method and system for authorizing access to resources requested by a first user. To begin the process, the first user submits an ID of the first user as an individual requesting access to one of the resources. The first user is also a member of a group comprising a plurality of individual users. The user ID is authenticated although the authentication process is not part of the present invention. The present invention includes various tables and programs involved in the authorization process. A first table indicates at least one group of a plurality of individual users. A second table indicates which resources are accessible by which of the users and which resources are accessible by which of the groups. An authorization program compares the first user to entries in the first table to determine which group or groups the first user is a member. Next, the authorization program compares the first user and the group or groups in which the first user is a member to entries in the second table to determine which resources the first user is authorized to access. Thus, the resources that the user ID is authorized to access are based not only on the user as an individual, but the group in which the user is a member.

Brief Description of the Drawings

Figure 1 is a block diagram illustrating components of the present invention.

Figures 2a-e illustrate in more detail a cross-referencing authorization data base of Figure 1.

Figure 3 illustrates in more detail a resource authorization data base of Figure 1.

Figure 4 is a flow chart illustrating operation and implementation of the present invention.

Detailed Description of the Preferred Embodiments

Referring now to the figures in detail, wherein like reference numbers indicate like elements throughout, Figure 1 illustrates a computer system or network generally designated 10 according to the present invention. Network 10 comprises multiple clients 14a,b,...n in the form of programmed personal computers or terminals, a common server computer 16, a resource data base 17, an authentication data base 20, a cross-referencing authorization data base 22 and a resource authorization data base 24. In the illustrated embodiment, the resource data base 17 is shown as being stored on a single, external disk drive, although the resource data base can be stored on multiple disk drives, external or internal to the server. The resource data base 17 may store data, computer programs or other resources. Each client 14a, b,...n is operated by a respective (human) user 12a, b,...n. The server can access any of the data bases 17, 20, 22 and 24 on behalf of a user. Figure 1 also illustrates an authentication program 15, an authorization program 19 and a resource management program 21 within the server 16.

The authentication data base 20 includes an authentication table. The authentication table includes in a first column a list of IDs of (individual) users or groups, and in a second column a valid password for each ID. All IDs in the authentication system are typically associated with the name of the authentication data base such as the name of a corporation that issued the IDs. If a user submits a valid user ID and matching password from an authentication data base that the server recognizes, then the user is authenticated and can log-on or establish a session with server 16.

Figure 2 illustrates the cross-referencing authorization data base 22 in more detail. The cross-referencing data base includes tables 22a-e storing IDs and ID related information for individuals and groups. By way of example, Table 22a contains user ID information for selected individuals from IBM corporation. The first column of Table 22a lists user IDs (including the authenticating data base name) for individuals, for example rsmith@IBM.com, tjones@IBM.com, and bjohnson@IBM.com. The second column of Table 22a lists the corresponding user description including the user's name, organization and company. (In this example, the corporation is divided into different organizations, by location or department.) Table 22a lists in the second column, Robert Smith from Main organization of IBM, Thomas Jones from Main organization of IBM, and Betty Johnson from Main organization of IBM. Thus, Robert Smith from Main organization of IBM is the user who submits user ID rsmith@IBM.com. Likewise, Thomas Jones from Main organization of IBM is the user who submits user ID tjones@IBM.com and Betty Johnson from Main organization of IBM is the user who submits user ID bjohnson@ IBM.com.

Table 22b contains group IDs and related information for various groups of individual users. The first column of Table 22b lists group IDs (including the authenticating data base name), for example, Progroup from IBM and Tesgroup from IBM. The second column of Table 22b lists the corresponding group description, including the name of the group, organization and company, for example, Programmer_Main_IBM meaning the Programmer group from Main

organization of IBM. The third column of Table 22b lists the descriptions of the individuals, by name, organization and company, who are members of the corresponding group. For example, Robert Smith of Main organization and IBM company, Thomas Jones of Main organization and IBM company and Betty Johnson of Main organization and IBM company are all members of the Programmer group.

Table 22c contains additional user information for rsmith@IBM.com and user information for three additional individual users. Table 22c has the same format as Table 22a. The user descriptions from Table 22c have different organization components than the user descriptions from Table 22a. The user descriptions from Table 22c include an Elm or Oak component whereas the user descriptions from Table 22a all include a Main component. It should be noted that the same user ID, rsmith@IBM.com appears in both Tables 22a and 22c and represents the same person, although the user description recorded in the second column of each table is different. Table 22a lists Robert Smith_Main_IBM whereas Table 22c lists Robert Smith_Elm_IBM. As explained in more detail, in the illustrated embodiment of the present invention, the entire user description forms an entry in the authorization data base.

Table 22d contains additional group information for Progroup@IBM.com and group information for an additional group, Debgroup@IBM.com. Table 22d has the same format as Table 22b. The group descriptions from Table 22d have different organization components than the group descriptions from Table 22b. The group descriptions from Table 22d include an Elm or Oak component whereas the group descriptions from Table 22b include a Main component.

Table 22e contains an additional user ID on a different system for Robert Smith and user information for one additional individual. Table 22e has the same format as Table 22a. The user descriptions from Table 22e have different organization components than the user descriptions from Table 22a. The user descriptions from Table 22e include an Oak or North component whereas the user descriptions from Table 22a include a Main component. It should be noted that

the same person, Robert Smith, has a different user ID and user description in Table 22e than in Table 22a.

Figure 3 illustrates the Resource Authorization data base 24 in more detail. The Resource Authorization data base includes a table indicating which user descriptions and which group descriptions are authorized to access which resources. The first column of the table lists the user descriptions and group descriptions and the second column lists the resources that each user description or group description is authorized to access. For example, Robert Smith_Main_IBM is authorized to access Customer data, Robert Smith_Elm_IBM is authorized to access Schedule data, Thomas Jones_Main_IBM is authorized to access Schedule data, Betty Smith_Main_IBM is authorized to access Finance data, ProGroup_Main_IBM is authorized to access Program Functions data, Programmer_Elm_IBM is authorized to access Program Requirements data, Debug_Oak_IBM is authorized to access Problem Report data, etc. Even though the individual members of each group are authorized to access the data available to the Group ID, the Resource Authorization table 24 does not include an index for each of the members of the group to the data accessible to their group. For example, even though Carol Parker_Elm_IBM is a member of the Programmer_Elm_IBM, Resource Authorization table 24 does not indicate that Carol Parker_Elm_IBM has access to the Program Requirements data. It should be noted that the Resource Authorization table does not include an index for user IDs or group IDs. Also, in the illustrated embodiment of the Resource Authorization table and the authorization program described below, access is based on the entire user description or group description, not just the user name or group name. However, if desired access could be based on the user name or group name without the organization component or the company component.

Figure 4 illustrates the authentication program 15 (Steps 50 and 52) and authorization program 19 (Steps 56, 58, 60, 62, 68, 70, 80) within server 16 in more detail. User 12a, acting through client 14a, attempts to log-on or establish a session with the server 16 by entry of the ID and password of the user at the client along with an indication that a log on or session with the

server is requested. The ID can be that of an individual or a group. However, in this first example, assume the ID is from an individual user, rsmith@IBM.com. (Step 50) In response, the authentication program 15 within server checks for this combination of user ID and password in the authentication table of data base 20 to determine if they match. (Step 52) (Other authentication techniques are also known and usable and are not considered part of the present invention. For example, a process involving a digital certificate can be used to indicate authenticity.) Assuming the user ID is authenticated, the user next requests access to a specific resource such as Program Requirements data. In response, the user ID is passed to the authorization program 19 along with the request for the specified resource. (Step 56) (It is also possible that the authentication program at this time can substitute another, unique ID for the ID that was submitted by the user. If so, the following explanation of the present invention applies to the substitute user ID.) The authorization program determines that the ID is a user ID. (Decision 58) Next, the authorization program reads the first column of tables 22a,c,e, searching for this user ID. The authorization program will identify the first row of Table 22a and the first row of Table 22c. Table 22a indicates that rsmith@IBM.com is the user ID for Robert Smith_Main_IBM and Table 22c indicates that rsmith@IBM.com is the user ID for Robert Smith_Elm_IBM. (Step 60). Next, the authorization program 19 searches for any groups in which Robert Smith_Main_IBM or Robert Smith_Elm_IBM is a member. Thus, authorization program 19 next reads the third column of Tables 22b and 22d, searching for either of these user descriptions. Authorization program identifies the first row in Table 22b for Programmer_Main_IBM, and the first row of Table 22d for Programmer_Elm_IBM. (Step 62). It should be noted that the authorization program 19 did not identify the second row of Table 22d for Debug_Oak_IBM because this group includes a different user description, Robert Smith_Oak_IBM, for the same person, Robert Smith. At this point, the authorization program has determined that the user ID rsmith@IBM.com is authorized to access data accessible to Robert Smith_Main_IBM, Robert Smith_Elm_IBM, Programmer_Main_IBM and Programmer_Elm_IBM.

Next, the authorization program searches down the Resource Authorization table to attempt to locate a row containing the name of the requested data (in the second column) and the descriptions of the users and groups (in the first column) identified in steps 60 and 62. In the foregoing example, the entities identified in steps 60 and 62 are Robert Smith_Main_IBM, Robert Smith_Elm_IBM, Programmer_Main_IBM and Programmer_Elm_IBM and the requested data is Program Requirements. (Step 68) In the illustrated example, the authorization is found in the sixth row. Therefore, the authorization program concludes that the request by user ID rsmith@IBM.com to access the Program Requirements data should be granted (even though the entries in the Resource Authorization table for Robert Smith_Main_IBM and Robert Smith_Elm_IBM do not indicate authorization to access the Program Requirements data). Next, the authorization program notifies Resource Management Program 21 that the request by rsmith@IBM.com to access the Program Requirements data should be granted. (Step 70) Finally, the server downloads the Program Requirements data to the client 14a so that the user 12a can access the Program Requirements data.

Referring again to step 50, assume in this next example that the user submits an ID of the user as an individual such as rsmith@IBM.com and then another ID of a group in which the user is a member, such as Debgroup@IBM.com. In response, the authentication program 15 within server checks for this combination of individual user ID and associated password and this combination of group ID and associated password in the authentication table of data base 20 to determine if both sets match. (Step 52) Assuming both sets match, the individual user ID and the group ID are considered authenticated.

Next, the user requests access to a specific resource such as Problem Reports data. (Step 56) For purposes of explanation, the handling of this request by the authorization program can be viewed as processing part of the request based on the individual user ID and processing the other part of the request based on the group ID to determine if either processing yields the requested authorization. The authorization program processes the part of the request based on

the individual user ID, rsmith@IBM.com, in steps 60, 62, 68 and 70 as described above (when the individual user ID is submitted without any group ID). However, the processing of this part of the request based on the individual user ID will not yield authorization to access the Problem Reports data as explained above. However, the processing of the other part of the request based on the group ID in steps 80, 68 and 70 will yield authorization to access the Problem Reports data, as follows. The authorization program reads the first column of tables 22b,d searching for this group ID. The authorization program will identify the second row of Table 22d. Table 22b indicates that Debgroup@IBM.com is the group ID for Debug_Oak_IBM. (Step 80). Thus, the authorization program has determined that the group ID Debgroup@IBM.com is authorized to access data accessible to Debug_Oak_IBM, and none other. Next, the authorization program searches down the Resource Authorization table to attempt to locate a row where Debug_Oak_IBM is listed in the first column and the requested data, Problem Report data, is listed in the second column. (Step 68). (As explained above, pursuant to the submission of the individual user ID, rsmith@IBM.com, the authorization program also searched down the Resource Authorization table to attempt to locate a row where Robert Smith_Main_IBM, Robert Smith_Elm_IBM, Programmer_Main_IBM or Programmer_Elm_IBM is listed in the first column and Problem Report data was listed in the second column, but this was unsuccessful.) In the illustrated example, the seventh row lists Debug_Oak_IBM in the first column and the requested data, Problem Report data, in the second column. Therefore, the authorization program concludes that the request by the combination of user ID rsmith@IBM.com and group ID Debgroup@IBM.com to access the Problem Reports data should be granted and notifies Resource Management Program 21. (Step 70) Finally, the server downloads the Problem Reports data to client 14a so that the user can access the Problem Reports data.

Based on the foregoing, a system and method for determining which resources a user can access based on user IDs or group IDs have been disclosed in accordance with the present invention. However, numerous modifications and substitutions can be made without deviating from the scope of the present invention. For example, the Resource Authorization table could

also be indexed by user ID and group ID instead of user description and group description. Also, other user IDs, groups of users and group IDs can and will be included in the tables of data base 22. Therefore, the present invention has been disclosed by way of illustration and not limitation, and reference should be made to the following claims to determine the scope of the present invention.

Docket No. END920010126US1